ON THE GENERALISED TATE CONJECTURE FOR PRODUCTS OF ELLIPTIC CURVES OVER FINITE FIELDS

BRUNO KAHN

ABSTRACT. We prove the generalised Tate conjecture for H^3 of products of elliptic curves over finite fields, by slightly modifying the argument of M. Spiess [7] concerning the Tate conjecture. We prove it in full if the elliptic curves run among at most 3 isogeny classes. We also show how things become more intricate from H^4 onwards, for more that 3 isogeny classes.

Let $\mathbf{F}_q$ be a finite field. It is known that the Tate conjecture for all smooth projective varieties over $\mathbf{F}_q$ implies the generalised Tate conjecture for all smooth projective varieties over $\mathbf{F}_q$ ([3, Rk. 10.3 2)], [6, §1]); however, the proofs in these two references are non-effective. It is therefore of interest to ask if one can prove the generalised Tate conjecture for certain explicit classes of $\mathbf{F}_q$-varieties.

In [7], Michael Spiess proved the Tate conjecture for products of elliptic curves over a finite field: this provides a natural candidate for such a class. In this note, we show that a slight modification of his argument does yield the generalised Tate conjecture, in cohomological degree 3 or if the elliptic curves run over at most 3 distinct isogeny classes.

Contrary to [3] and [6], the proofs do not appeal to Honda's existence theorem [1]. This theorem appears, however, when studying H^4 of a well-chosen product of 4 elliptic curves: this is directly related to the delicate combinatorics of Weil numbers[1]; we illustrate the non-effectiveness of the arguments from [3] and [6] in this case.

Theorem 1. *Let X be a product of elliptic curves over $\mathbf{F}_q$. Then the generalised Tate conjecture holds for $H^3(\bar{X}, \mathbf{Q}_l)$: the subspace of Tate coniveau 1 coincides with the first step of the coniveau filtration.*

Let $q = p^r$ for p be a prime number and $r \geq 1$. As in [7], we write $[\rho]$ for the ideal generated by an algebraic integer ρ. As in [7, Def.

Date: Jan. 7, 2011.

[1]The corresponding computation seems in contradiction with the one from [4, Claim p. 130].

1], we also say that a Weil q-number α is *elliptic* if it arises from the Frobenius endomorphism of an elliptic curve over $\mathbf{F}_q$. There are two kinds of elliptic Weil q-numbers: the supersingular ones, of the form $\pm p^{r/2}$ and the ordinary ones, which generate a quadratic extension of $\mathbf{Q}$ in which p is totally decomposed. In the latter case, if $[p] = \mathfrak{p}_1\mathfrak{p}_2$, then

$$[\alpha] = \mathfrak{p}_1^r \text{ or } \mathfrak{p}_2^r \tag{1}$$

(compare [7, Lemma 2].)

The main lemma is:

Lemma 2. *Let $\alpha_1, \alpha_2, \alpha_3$ be 3 elliptic Weil q-numbers, generating a multiquadratic number field $K/\mathbf{Q}$. Suppose that*

$$[\alpha_1\alpha_2\alpha_3] = [q\beta]$$

with β an algebraic integer. Then there exist $i \neq j$ such that

$$[\alpha_i\alpha_j] = [q].$$

Proof. If two of the α_i are supersingular the assertion is obvious. Thus we may assume that at least two of the α_i are ordinary.

Case 1: one of the α_i, say α_3, is supersingular. If $[\alpha_1\alpha_2] \neq [q]$, one sees that $[\alpha_1\alpha_2]$ is not divisible by $[p]$. (Using (1) as in [7, proof of Lemma 3], either α_1 and α_2 generate the same quadratic field and then $[\alpha_1] = [\alpha_2]$, or α_1 and α_2 generate a biquadratic extension $K/\mathbf{Q}$ in which $[p] = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$ and then without loss of generality, $[\alpha_1] = (\mathfrak{q}_1\mathfrak{q}_2)^r$ and $[\alpha_2] = (\mathfrak{q}_1\mathfrak{q}_3)^r$.) If $r > 1$, we get a contradiction. If $r = 1$, we have the equation $[\alpha_1\alpha_2] = [\sqrt{p}\beta]$ in $K(\sqrt{p})$. Since p is totally ramified in $\mathbf{Q}(\sqrt{p})$, the prime divisors of $[p]$ in K are totally ramified in $K(\sqrt{p})$ and we get a new contradiction.

Case 2: all the α_i are ordinary. We assume again that the conclusion of the lemma is violated, and show that $[\alpha_1\alpha_2\alpha_3]$ is then not divisible by $[p]$.

If (say) α_1 and α_2 generate the same quadratic field, then as seen in Case 1, $[\alpha_1] = [\alpha_2]$ and $[\alpha_1\alpha_2\alpha_3]$ is not divisible by $[p]$. Suppose now that the α_i generate three distinct imaginary quadratic fields. In particular, $[K : \mathbf{Q}] \geq 4$. If $[K : \mathbf{Q}] = 4$, then $K = \mathbf{Q}(\alpha_1, \alpha_2)$ (say) and α_1, α_2 generate two distinct quadratic subextensions of K. Then α_3 must generate the third quadratic subextension: but this is impossible because the latter is real. Thus $[K : \mathbf{Q}] = 8$.

We now set up some notation. Let $G = Gal(K/\mathbf{Q}) \simeq (\mathbf{Z}/2)^3$, and let $X(G)$ be the character group of G. The quadratic subextensions generated by $\alpha_1, \alpha_2, \alpha_3$ correspond to characters χ_1, χ_2, χ_3 forming a basis of $X(G)$. Let $(\sigma_1, \sigma_2, \sigma_3)$ be the dual basis of G. Finally, let

$c \in G$ be the complex conjugation: since $\chi_i(c) = 1$ for all i, we find that $c = \sigma_1\sigma_2\sigma_3$. Note that, since the α_i are Weil q-numbers, we have $\alpha_i\alpha_i^c = q$.

Since p is totally decomposed in all $\mathbf{Q}(\alpha_i)$, it is totally decomposed in K. Pick a prime divisor $\mathfrak{p}$ of $[p]$. We then have

$$[p] = \mathfrak{p}^{\sum_{\sigma\in G}\sigma}.$$

Since α_1 is invariant under σ_2 and σ_3, we find from (1), up to changing α_1 to α_1^c:

$$[\alpha_1] = \mathfrak{p}^{r(1+\sigma_2)(1+\sigma_3)}$$

and similarly:

$$[\alpha_2] = \mathfrak{p}^{r(1+\sigma_1)(1+\sigma_3)}, \quad [\alpha_3] = \mathfrak{p}^{r(1+\sigma_1)(1+\sigma_2)}.$$

We now compute: $[\alpha_1\alpha_2\alpha_3] = \mathfrak{p}^{rm}$, with

$$\begin{aligned} m &= (1+\sigma_2)(1+\sigma_3) + (1+\sigma_1)(1+\sigma_3) + (1+\sigma_1)(1+\sigma_2) \\ &= 3 + 2(\sigma_1+\sigma_2+\sigma_3) + \sigma_2\sigma_3 + \sigma_1\sigma_3 + \sigma_1\sigma_2. \end{aligned}$$

This shows that $\mathfrak{p}^{rm}$ is not divisible by $[p]$ (the summand $\sigma_1\sigma_2\sigma_3$ is missing). Similarly, $[\alpha_1\alpha_2\alpha_3^c] = \mathfrak{p}^{rm'}$ with

$$\begin{aligned} m' &= (1+\sigma_2)(1+\sigma_3) + (1+\sigma_1)(1+\sigma_3) + c(1+\sigma_1)(1+\sigma_2) \\ &= 2 + \sigma_1 + \sigma_2 + 3\sigma_3 + 2\sigma_1\sigma_3 + 2\sigma_2\sigma_3 + \sigma_1\sigma_2\sigma_3 \end{aligned}$$

and $\mathfrak{p}^{rm'}$ is not divisible by $[p]$ (the summand $\sigma_1\sigma_2$ is missing). The other possible products reduce to those by permutation of the α_i and conjugation by c: the proof is complete. □

Proof of Theorem 1. It is sufficient to prove the equality after tensoring with a large enough number field K, Galois over $\mathbf{Q}$. We first observe that the Frobenius action on $H^*(\bar{X}) := H^*(\bar{X}, \mathbf{Q}_l) \otimes K$ is semi-simple since X is an abelian variety (compare [2, Lemma 1.9]). Let v be an eigenvector of Frobenius, with eigenvalue ρ. Since $H^3(\bar{X}) = \Lambda^3 H^1(\bar{X})$ and X is a product of elliptic curves, v is a sum of vectors of the form $v_1 \wedge v_2 \wedge v_3$ where $v_i \in H^1(\bar{X})$ is an eigenvector with Frobenius eigenvalue α_i with $\alpha_1\alpha_2\alpha_3 = \rho$, α_i corresponds to an elliptic curve E_i and v_i comes from $H^1(\bar{E}_i) \hookrightarrow H^1(\bar{X})$.

Suppose ρ is divisible by q. Without loss of generality, we may assume that v is a single vector $v_1 \wedge v_2 \wedge v_3$. By Lemma 2, up to renumbering we have $[\alpha_1\alpha_2] = [q]$. As in [7, Corollary p. 288], there is an integer $N \geq 1$ such that $(\alpha_1\alpha_2)^N = q^N$.

By the Tate conjecture in codimension 1 for $E_1 \times E_2$ (Deuring, cf. Tate [8]), $v_1 \wedge v_2 \otimes \mathbf{Q}_l(1) \in H^2(\bar{E}_1 \times \bar{E}_2)(1)$ is of the form $\mathrm{cl}(\gamma)$ where

γ is a cycle of codimension 1 on $\bar{E}_1 \times \bar{E}_2$ and cl is the cycle class map. Hence $v \otimes \mathbf{Q}_l(1) = \mathrm{cl}(\pi^*\gamma) \cdot v_3$, with $\pi : X \to E_1 \times E_2$ the projection. □

Theorem 3. *Let X be a product of elliptic curves, belonging to at most 3 distinct isogeny classes. Then the generalised Tate conjecture holds for X in all degrees and all coniveaux.*

The proof is a variant of the one above: in the proof of Lemma 2, Case 2, the computation showing that $[\alpha_1\alpha_2\alpha_3]$ and $[\alpha_1\alpha_2\alpha_3^c]$ are not divisible by $[p]$ extends to show that $[\alpha_1^{n_1}\alpha_2^{n_2}\alpha_3^{n_3}]$ and $[\alpha_1^{n_1}\alpha_2^{n_2}(\alpha_3^c)^{n_3}]$ are not divisible by $[p]$ for any nonnegative integers n_1, n_2, n_3. This generalises Lemma 2 to any product of Weil q-numbers involved in the cohomology of X. □

Finally, we show what problems arise when one tries to replace 3 by 4 in Theorem 1 or 3. Start again with three non isogenous ordinary elliptic curves E_1, E_2, E_3, with Weil numbers $\alpha_1, \alpha_2, \alpha_3$. We retain the notation from Case 2 in the proof of Lemma 2. Apart from χ_1, χ_2 and χ_3,

$$\chi_1\chi_2\chi_3$$

is the unique character which does not vanish on c. In the corresponding quadratic subfield of K, there is the possibility of a new Weil q-number α_4 with

$$[\alpha_4] = \mathfrak{p}^{r(1+\sigma_1\sigma_2)(1+\sigma_1\sigma_3)}.$$

This can actually be achieved provided r is large enough. Since the class group $Cl(O_K)$ is finite, we may choose r such that $\mathfrak{p}^r$ is principal, say $\mathfrak{p}^r = [\lambda]$. Then $N_{K/\mathbf{Q}}(\lambda) = q$ (since K is totally imaginary) and we choose $\alpha_4 = \lambda^{(1+\sigma_1\sigma_2)(1+\sigma_1\sigma_3)}$.

Up to increasing r, we may assume that the similar formulas hold for α_1, α_2 and α_3.

By Honda's theorem [1], α_4 corresponds to a 4th (isogeny class of) elliptic curve E_4. Now $\alpha_1\alpha_2\alpha_3\alpha_4^c = \lambda^{m''}$ with

$$\begin{aligned} m'' &= m + c(1+\sigma_1\sigma_2)(1+\sigma_1\sigma_3) \\ &= 3 + 2(\sigma_1+\sigma_2+\sigma_3) + \sigma_2\sigma_3 + \sigma_1\sigma_3 + \sigma_1\sigma_2 \\ &\quad + \sigma_1\sigma_2\sigma_3(1 + \sigma_1\sigma_2 + \sigma_1\sigma_3 + \sigma_2\sigma_3) \\ &= N + 2(1 + \sigma_1 + \sigma_2 + \sigma_3) \end{aligned}$$

with $N = \sum_{\sigma \in G} \sigma$. Thus $\alpha_1\alpha_2\alpha_3\alpha_4^c = q\beta^2$, with

$$\beta = \lambda^{(1+\sigma_1+\sigma_2+\sigma_3)}.$$

This β is a new Weil q-number; it generates K since the isotropy group of $[\beta]$ in G is trivial. By the Honda-Tate theorem, it corresponds

to the isogeny class of a simple $\mathbf{F}_q$-abelian variety A of dimension 4 (see [8, p. 142 formula (7)]).

Let us say that a Weil q-number γ is *ordinary* if $\gcd(\gamma, \gamma^c) = 1$. This is equivalent to requiring that $\gcd(p, \gamma + \gamma^c) = 1$, hence, by [9, Prop. 7.1], that the corresponding abelian variety be ordinary. Let $\gamma \in K$ be an ordinary Weil q-number. Since $\gamma\gamma^c = q$, the divisor of γ is of the form $\mathfrak{p}^{rm_\gamma}$, where $m_\gamma \in \mathbf{Z}[G]$ is the sum of elements in a section of the projection $G \to G/\langle c\rangle$. These sections form a torsor under the group of maps from $G/\langle c\rangle$ to $\langle c\rangle$, so there are 16 of them. Up to conjugation by c, we get 8. Among these 8, 4 are given by the kernels of the characters χ_1, χ_2, χ_3 and $\chi_1\chi_2\chi_3$, recovering $\alpha_1, \alpha_2, \alpha_3$ and α_4. Among the 4 remaining ones, there is the one defining β; since the isotropy group of $[\beta]$ is trivial, the other ones are conjugate to it. We have exhausted the ordinary Weil q-numbers contained in K.

Let $X = \prod_{i=1}^4 E_i$. If we run the technique of proof of [3] or [6] to try and prove the generalised Tate conjecture for $N^1H^4(\bar{X})$, we end up with a Tate cycle in $H^6(\bar{X} \times \bar{A})(3)$. This Tate cycle is exotic in the sense that it is not a linear combination of products of Tate cycles of degree 2 (cf. [5, p. 136]), because the relation

$$\alpha_1\alpha_2\alpha_3\alpha_4^c(\beta^2)^c = q^3$$

cannot be reduced to relations of degree 2. I have no idea if the Tate conjecture can be proven for $X \times A$. Can the methods of [5] be used to answer this question?

Acknowledgements. Most of this work was done during a stay at IMPA (Rio de Janeiro) in November 2010, in the framework of the France-Brazil cooperation. I thank the first for its hospitality and the second for its support.

References

[1] T. Honda *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968) 83–95.

[2] B. Kahn *Équivalences rationnelle et numérique sur certaines variétés de type abélien sur un corps fini*, Ann. Sci. Éc. Norm. Sup. **36** (2003), 977–1002.

[3] B. Kahn *Zeta functions and motives*, Pure Appl. Math. Quarterly **5** (2009), Special Issue: In honor of Jean-Pierre Serre, 507–570 [2008].

[4] E. Kowalski *Some local-global applications of Kummer theory*, Manuscripta Math. **111** (2003), 105–139.

[5] J.S. Milne *The Tate conjecture for certain abelian varieties over finite fields*, Acta Arithm. **100** (2001), 135–166.

[6] J.S. Milne, N. Ramachandran *Motivic complexes over finite fields and the ring of correspondences at the generic point*, Pure Appl. Math. Q. **5** (2009), Special Issue: In honor of John Tate, 1219–1252.

[7] M. Spiess *Proof of theTate conjecture for products of elliptic curves over finite fields*, Math. Ann. **314** (1999), 285–290.
[8] J.T. Tate *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1965), 134–144.
[9] W.C. Waterhouse *Abelian varieties over finite fields*, Ann. Sci. ENS **2** (1969), 121–160.

Institut de Mathématiques de Jussieu, UPMC - UFR 929, Mathématiques, 4 Place Jussieu, 75005 Paris, France
E-mail address: kahn@math.jussieu.fr